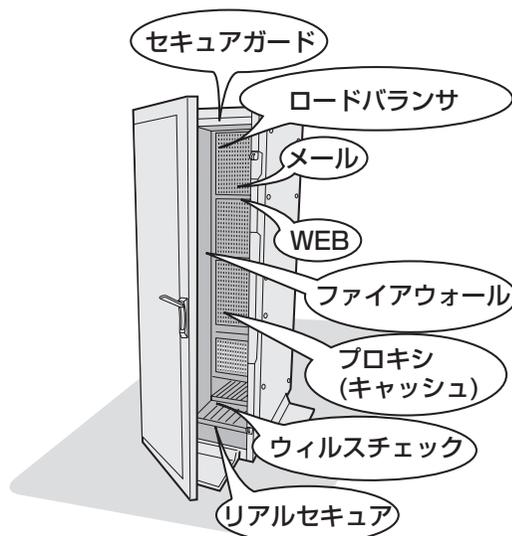
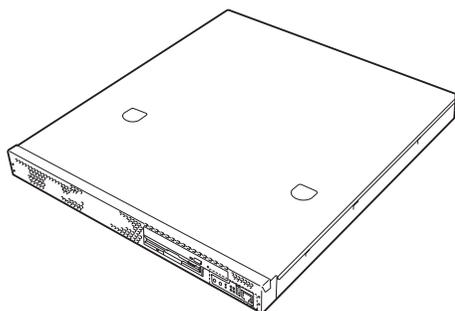
1 InterSec シリーズについて

本製品や添付のソフトウェアの特長、導入の際に知っておいていただきたい事柄について説明します。

InterSecシリーズとは

「オール・イン・ワン」から「ビルドアップ」へ。
お客様の運用目的に特化した設計で、必要のないサービス/機能を省き、セキュリティホールの可能性を低減し、インターネットおよびイントラネットの構築時に不可欠なセキュリティについて考慮して設計されたインターネットセキュリティ製品です。

1台のラックにそれぞれの機能を持つ装置を搭載(卓上設置も可能、またクラスタ構成可能)

InterSecシリーズの主な特長と利点は次のとおりです。

- **省スペース**

  設置スペースを最小限に抑えたコンパクトな筐体を採用。

- **運用性**

  運用を容易にする管理ツール。

- **クイックスタート**

  ウィザード形式の専用設定ツールを標準装備。短時間でセットアップを完了します。

- **高い拡張性**

  専用機として、機能ごとに単体ユニットで動作させているために用途に応じた機能拡張が容易に可能です。また、複数ユニットでクラスタ構成にすることによりシステムを拡張していくことができます。

- **コストパフォーマンスの向上**

  運用目的への最適なチューニングが行えるため、単機能の動作において高い性能を確保できます。また、単機能動作に必要な環境のみ提供できるため、余剰スペックがなく低コスト化が実現されます。

- **管理の容易性**

  環境設定や運用時における管理情報など、単機能が動作するに必要な設定のみです。そのため、導入・運用管理が容易に行えます。

InterSecシリーズには、目的や用途に応じて次のモデルが用意されています。

- **SGシリーズ(ファイアウォール)**

  インターネットと接続した中小規模の企業ネットワークを外部からの不正なアクセスから守るファイアウォール専用機です。

- **FWシリーズ(ファイアウォール)**

  CheckPoint FireWall-1を搭載し、高度なアクセス制御が可能な、大中規模の企業ネットワーク向けのファイアウォール専用機です。

- **LBシリーズ(ロードバランサ)**

  複数台のWebサーバへのトラフィック(要求)を整理し、負荷分散によるレスポンスの向上を目的とした装置です。

- **MWシリーズ(メール/WEB)**

  WebやFTPのサービスやインターネットを利用した電子メールの送受信や制御などインターネットで必要となるサービスを提供する装置です。

- **CSシリーズ(プロキシ)**

  Webアクセス要求におけるプロキシでのヒット率の向上(フォワードプロキシ)、Webサーバの負荷軽減・コンテンツ保護(リバースプロキシ)を目的とした装置です。

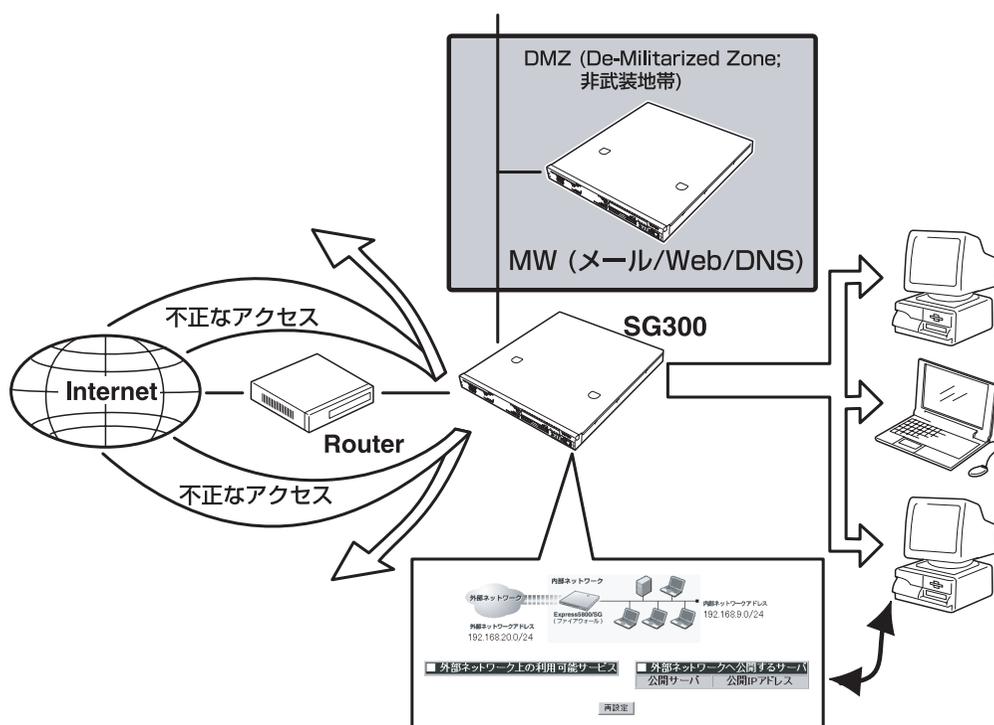
- **VCシリーズ(ウィルスチェック)**

  インターネット経由で受け渡しされるファイル(電子メール添付のファイルやWeb/FTPでダウンロードしたファイル)から各種ウィルスを検出/除去し、オフィスへのウィルス侵入、外部へのウィルス流出を防ぐことを目的とした装置です。

Express5800/SG300について

本装置の概略と運用に必要な情報を記します。

概　要

Express5800/SG300は、NEC独自のファイアウォールエンジンを搭載し、Virtual Private Network(VPN)機能、ホスト型IDS機能を装備したセキュリティアプライアンス機器です。
内部ネットワーク(社内LANなど)と外部ネットワーク(インターネットなど)との間のアクセスを制御し、外部からの不正な侵入を防ぎます。さらに、VPN機能による通信の暗号化やユーザ認証などを使って、インターネットなどの公衆のネットワーク上に、仮想的なユーザ専用のネットワークを実現することを可能にします。
設定・運用・管理をManagement Console(WEBベースGUI)に集約することで容易で迅速な導入を実現し、設置したその日から安全なネットワーク環境を提供します。

Management Consoleを利用してかんたんに
ポリシーを作成・編集し、セキュリティを強化可能

Express5800/SG300が提供するファイアウォールの特徴は次のとおりです。

- **アクセス制御**

  ステートフルインスペクション(通信を行うときだけ必要なポートを開く機能)により、高度なアクセス制御を可能とし、ユーザのセキュリティポリシに沿ったセキュアなネットワークを実現します。

- **アドレス変換機能(NAT/NAPT)**

  外部ネットワークと内部ネットワークとの相互通信を可能とするため、アドレス変換機能を実現しています。

- **通信量制限機能**

  ネットワークインターフェースごとに、通過するパケットの総量を制限することが可能です。これにより、アクセス過多によるサーバをダウンさせるDoS(Denial of Services)・DDoS(Distributed Denial of Services)などの攻撃が行われた場合にも、パケット量を制限し、サーバがダウンすることを防止します。

- **不正アクセス対策**

  — オートディフェンス機能

  攻撃者は、ウェブサーバやメールサーバの持つ脆弱性をついた攻撃を行う前に、どのサーバでどのサービスが稼動しているか事前に調査(ポートスキャン)しますが、Express5800/SG300ではその事前調査活動を検出し、あたかもウェブサーバやメールサーバが数多く存在するかのように応答し、実際にサービスが稼動しているサーバの発見を困難にさせることが可能です。さらに検出後、そのホストからのアクセスを一定時間すべて破棄します。

  — ステルススキャン検出機能

  ステルススキャンはポートスキャンと同様に、不正侵入のための前準備として行われます。通常ログなどに形跡を残さないためその発見が困難となります。Express5800/SG300では、ステルススキャン特有の正常でない通信を検出し、該当パケットの破棄とログを出力することが可能です。

  — Ping Sweep対策機能

  不正侵入のための前準備として、どのようなホストが稼動しているか調査するために、Ping Sweepなどが行われます。Ping Sweepは、ある範囲のIPアドレス宛にpingを送出し、応答を確認することで、ホストの存在を調査するものです。Express5800/SG300では、Ping Sweepを検出し、該当パケットの破棄とログを出力することが可能です。

  — SYN Flood対策機能

  SYN Floodは、DoS攻撃の一種で、サーバのリソースを消費し、サービスの提供をできなくする攻撃です。Express5800/SG300では、SYN Flood攻撃を検出しログを出力します。この機能により、ターゲットとなったホストを守ることが可能です。

  — IP Spoofing対策機能

  IP Spoofingは、パケットの発信元を詐称する手法です。不正なアクセスを、あたかも内部からの許可されたアクセスであるかのように見せかけ、内部ホストに対する攻撃を可能にします。Express5800/SG300では、ルーティング情報などを元にIP Spoofingを検出し、該当パケットの破棄とログを出力することが可能です。

— tracerouteステルス機能

あるホストまでの経路や時間を確認するために一般的に使われるtracerouteコマンドにより、経路の途中にファイアウォールが存在することを確認できます。Express5800/SG300では、tracerouteコマンドに対してもその存在を隠すことが可能です。これにより、悪意を持ったクライアントから、攻撃の対象となる可能性を低減し自分自身も守ることが可能です。

- **ユーザ管理機能**

あらかじめ定められたユーザに対してのみに、ファイアウォール機能によって守られたサービスを公開するため、その許可されたユーザ情報の管理、およびファイアウォールを通過するためのユーザ認証を行います。

- **URLフィルタリング機能**

あらかじめURLを設定しておくことで、そのWebサイトへのアクセスを制限できます。これによりインターネット上の好ましくないWebサイトや業務に関係無いWebサイトへのアクセスをブロックし、教育環境・作業効率の向上が見込めます。

- **VPN機能**

VPNとは、インターネットのような公衆のネットワーク上に、仮想的なユーザ専用のネットワークを実現する仕組みです。これにより、公衆ネットワーク上で起こりうる、通信の盗聴・改ざん・なりすましなどの危険性を排除することが可能です。Express5800/SG300では、通信相手とのLAN間接続VPNを構築することが可能であり、安価にVPN網を実現し、セキュアな通信環境を実現できます。

- **Management Console**

基本的なネットワークの設定から、ファイアウォールのセキュリティポリシの設定まで行うことのできる、統一されたウェブブラウザベースのユーザインターフェースです。

- **導入の容易性**

初期導入設定ツール、基本設定ツール、Management Console(かんたん設定/詳細設定)により、ファイアウォールなどを扱った経験の浅いユーザでも簡単に導入、運用を開始することができます。また、ネットワークインターフェースを4ポート装備しているので、ハードウェアの追加購入をすることなくDMZの構築が可能です。

- **ホットスタンバイ構成が可能**

二重化機能を標準でサポートしています。SG300を2台使用することでホットスタンバイ運用を実現し、可用性を高めます。

ライセンスキー

本製品を利用するためには、ライセンスキーの入手が必要となります。ライセンスキーを入手するためには、製品に同梱されているライセンス申請書に情報をご記入の上、ライセンス申請書に記載された宛先まで送付してください。約5営業日程度でe-mailにてライセンスキーを通知いたします。通知されたライセンスキーは重要な情報ですので、大切に保管してください。

ライセンスキーは、サポートサービス製品を購入いただき、サポートサービス申請をしていただく際にも必要な情報となります。

ソフトウェアサポートサービス

Express5800/SG300のソフトウェアおよびOSをサポートするためには以下の製品の購入が必須となります。

Exp58/SG（1年間）ソフトウェアサポートサービス

- **サービス内容**

Express5800/SG300のソフトウェアおよびOSについて、お客様(担当のNEC営業/SEを含む)からの電話、電子メールおよびFAXによる問い合わせを行うことができます。

また、インターネットを利用して、ソフトウェアおよびOSを利用可能な最新の状態へ無償でアップデートすることができます。

- **ハードウェア関するサービスは別途製品を手配いただく必要があります。**
- **ソフトウェアサポートサービスはオンサイトサービスを含んでおりません。**

- **サービス有効期間**

ユーザ登録完了後、1年間です。

ソフトウェアサポートサービスをご利用いただくには、初年度分からサポートサービス製品を手配していただく必要があります。

また、サービス有効期間終了後も継続してサービスを受けるためには、サポートサービス製品を再度ご購入いただく必要があります。

- **サービス受付時間**

弊社の営業日のうち、AM9:00～AM12:00・PM1:00～PM5:00です。

- **問い合わせ窓口のご案内**

お客様の登録が完了され次第、ご案内します。

● 問い合わせサポート範囲

Express5800/SG300にあらかじめインストールされているソフトウェアおよび添付されているNEC製のソフトウェアについてのお問い合わせに対応いたします。お客様の都合により、ソフトウェアを追加または変更した場合、本サービスの対象外となります。

● サービス開始手続き

サポートサービス製品に同梱されている「ソフトウェアサポートサービス申請書」に必要事項をご記入の上、Faxにて送付してください。申請書にはライセンスキーおよびサービス開始希望日を記入する欄などがあります。すべての項目がサービスを開始するにあたり必要な情報ですので漏れなくご記入ください。

お客様登録完了後、Express5800/SG300に投入するサポートキーおよび登録完了のお知らせが送付されます。

サポートサービスをご発注いただいてからお客様への導入時までのサービスは「暫定サポートサービス」としてサービスを提供させていただきます。ただし、暫定サポートサービス提供期間は最長3カ月とさせていただきます。

「ソフトウェアサポートサービス申請書」はお客様ごとに異なったものとなっており、複写しての使用はできません。

● 暫定サポートサービス

サポートサービス製品購入日から、ソフトウェアサポートサービス申請書にご記入いただいたサービス開始希望日までの間、暫定サポートサービスとして対応いたします。ただし、最長3カ月を限度として、技術的なQ&Aを提供します。

● サービス継続手続き

サービス有効期間(1年間)終了後もサービスを継続するためには、新規にサポートサービス製品を購入する必要があります。

また、継続のためにサポートサービス製品を購入いただいた場合には、サービス有効期間終了時にさかのぼって開始されます。前回の有効期間が切れる前にサポートサービスの購入を行ってください。

注意・制限事項

以下に示す注意・制限事項を確認の上、本装置を取り扱ってください。

- ソフトウェアアップデート機能を使用するには、ソフトウェアサポートサービスを購入し、有効なサポートキーを本製品に投入済みであることが必要です。
- ソフトウェアのアップデートを行うことで、設定画面等が本書の内容と異なる場合があります。その場合の操作方法についてはアップデート後のManagement Consoleのヘルプを参照してください。
- ユーザ認証の要求経路によって適用するルールを動的に変更することはできません。
- 設定管理用にブラウザの利用できる環境が必要です。以下のブラウザを推奨します。

  Microsoft Internet Explorer 6.0 SP1(日本語版・Windows版)
- ユーザ認証を行うには、ブラウザの利用できる環境が必要です。以下のブラウザを推奨します。

  Microsoft Internet Explorer 6.0 SP1(日本語版・Windows版)
- ユーザ認証時に、ユーザが利用している端末と本製品との間にソースアドレスを置き換えるゲートウェイが設置されている場合、そのゲートウェイを越えての認証はできません。
- システムの基本設定(インタフェースアドレス、ルーティング情報など)については必ずManagement Consoleの「基本設定」で行うか、またはシリアルコンソールからsgsetupコマンドを実行して変更してください。
- マルチキャスト通信には対応していません。
- リモートアクセスVPNにはいくつかの制限事項があります。詳細については弊社営業担当またはSEまでお問い合わせください。
- VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があるとVPN通信は行えません。
- 二重化構成でフェイルオーバが発生した場合、接続されていたセッションは切断されます。

添付のディスクについて

本装置にはセットアップや保守・管理の際に使用するCD-ROMやフロッピーディスクが添付されています。ここでは、これらのディスクに格納されているソフトウェアやディスクの用途について説明します。

重要 **添付のフロッピーディスクやCD-ROMは、システムの設定が完了した後でも、システムの再インストールやシステムの保守・管理の際に使用する場合があります。なくさないように大切に保管しておいてください。**

- バックアップCD-ROM

  システムのバックアップとなるCD-ROMです。

  バックアップCD-ROMには、システムのセットアップに必要なソフトウェアや各種モジュールの他にシステムの管理・監視をするための専用のアプリケーション「ESMPRO/ServerAgent」と「エクスプレス通報サービス」が格納されています。システムに備わったRAS機能を十分に発揮させるためにぜひお使いください。ESMPRO/ServerAgentの詳細な説明はバックアップCD-ROM内のオンラインドキュメントをご覧ください。エクスプレス通報サービスを使用するには別途契約が必要です。お買い求めの販売店または保守サービス会社にお問い合わせください。

- EXPRESSBUILDER(SE) CD-ROM

  本体およびシステムの保守・管理の際に使用するCD-ROMです。

  このCD-ROMには次のようなソフトウェアが格納されています。

  - EXPRESSBUILDER(SE)

    再セットアップの際に装置の維持・管理を行うためのユーティリティを格納するためのパーティション(保守パーティション)を作成したり、システム診断やオフライン保守ユーティリティなどの保守ツールを起動したりするときに使用します。詳細は5章を参照してください。

  - DianaScope

    システムが立ち上がらないようなときに、リモート(LAN接続またはRS-232Cケーブルによるダイレクト接続)で管理PCから本装置を管理する時に使用するソフトウェアです。詳細は5章を参照してください。

  - ESMPRO/ServerManager

    ESMPRO/ServerAgentがインストールされたコンピュータを管理します。詳細はEXPRESSBUILDER(SE)CD-ROM内のオンラインドキュメントを参照してください。

- 再インストール用ディスク(フロッピーディスク)

  再インストールの際に使用するフロッピーディスクです。なくさないよう、大切に保管しておいてください。

- 初期導入設定用ディスク(フロッピーディスク)

  Express5800/SG300の初期導入時の設定をするためのフロッピーディスクです。